AMENDMENTS TO THE CLAIMS:

1. (Currently Amended) A method of producing a digital certificate ~~during~~ in which a certification authority ~~groups~~ performs the steps of grouping together, in a data set, a public key and digital data comprising data identifying the proprietor of ~~the~~ said public key and of an associated private key, ~~and then signs~~ signing the data set in order to produce a digital certificate, and storing the signed data set in a computer-readable storage medium,

~~the method being characterised in that~~ wherein the digital data also comprise data identifying at least one of means of generating the private key, ~~and/or~~ means of storing the private key on a medium, ~~and/or~~ and means of signing with the private key.

2. (Original) A method according to claim 1, in which the data identifying the means of generating the private key comprise data identifying:

- a method of generating the private key and/or
- hardware on which the method of generating the private key is implemented, and/or
- a place on which the method of generating the private key is implemented.

3. (Currently Amended) A method according to claim 1 ~~or 2~~, in which the data identifying the means of storing the private key comprise data identifying:

- a method of storing the private key on a medium, and/or
- hardware on which the method of storing the private key is implemented, and/or
- a place on which the method of storing the private key is implemented, and/or
- a storage medium on which the private key is stored.

4. (Currently Amended) A method according to ~~one of claims 1 to 3~~ claim 1, in which the data identifying the signature means comprise data identifying:

- a signature method using the private key, and/or
- a memory medium on which ~~the~~ said signature method is stored.

5. (Currently Amended) A method according to ~~one of claims 2 to 4~~ claim 2, in which the data identifying hardware or a storage medium comprise:

- a reference identifying ~~the~~ said hardware or ~~the~~ said storage medium, and/or
- an identification of a manufacturer of ~~the~~ said hardware or of ~~the~~ said storage medium, and/or
- an indication of a security level of ~~the~~ said hardware or of ~~the~~ said storage medium defined according to a standard ISO 15408.

6. (Currently Amended) A method according to ~~one of claims 2 to 5~~ claim 2, in which the data identifying a method comprise:

- a reference identifying ~~the~~ said method, and/or
- an identification of an inventor of ~~the~~ said method, and/or
- an indication of a security level of ~~the~~ said method according to ISO 15408.

7. (Currently Amended) A method according to ~~one of claims 2 to 6~~, claim 2 in which the data identifying a place comprise:

- an identification of ~~the~~ said place, and/or
- an identification of a security level of ~~the~~ said place according to ISO 15408.

8. (Original) A digital certificate stored in a computer-readable medium, comprising:

- a public key,

- data identifying a proprietor of the public key and of an associated private key, and
- data identifying at least one of means of generating the private key, ~~and/or~~ means of storing the private key on a medium, ~~and/or~~ and means of signature with ~~the~~ said private key.

9. (Original) A certificate according to claim 8, of the X509 type according to a standard Information Technology – Open Systems Interconnection – The Directory : Public Key and Attribute Certificate Frameworks, dated March 2000, of the International Telecommunication Union, in which a set of predefined free fields are used to store the digital data identifying:

- a method of generating the private key, and/or
- hardware on which the method of generating the private key is implemented, and/or
- a place on which the method of generating the private key is implemented, and/or
- a method of storing the private key on a medium, and/or
- hardware on which the method of storing the private key is implemented, and/or
- a place on which the method of storing the private key is implemented, and/or
- a storage medium on which the private key is stored, and/or
- a signature method using the private key, and/or
- a storage medium on which the said signature method is stored.

10. (Currently Amended) A method of using a digital certificate according to ~~one of claims 8 or 9~~ claim 8, comprising the following steps ~~consisting of~~:

- receiving a message signed with a private key,
- reading, in the digital certificate, data identifying means of generating the private key and/or means of storing the private key on a medium and/or means of signing with the private key,

- deducing therefrom a probability of ~~the~~ said private key having been used by a legitimate proprietor of ~~the~~ said private key,
- according to ~~the~~ said probability, accepting or refusing the electronic message.

11. (Original) A method according to claim 10, in which the message is accepted solely if the probability of the said key having been used by its legitimate proprietor is greater than a predefined value.

12. (Original) A method according to claim 10, in which:

- the message is accepted if the probability is greater than a first value (VB1),
- a confirmation of the said message is requested if the probability is between the first value (VB1) and a second value (VB2) less than the first value, and
- the message is refused if the probability is less than the second value (VB2).

13. (New) A method according to claim 2, in which the data identifying the means of storing the private key comprise data identifying:

- a method of storing the private key on a medium, and/or
- hardware on which the method of storing the private key is implemented, and/or
- a place on which the method of storing the private key is implemented, and/or
- a storage medium on which the private key is stored.

14. (New) A method according to claim 2, in which the data identifying the signature means comprise data identifying:

- a signature method using the private key, and/or
- a memory medium on which said signature method is stored.

15. (New) A method according to claim 3, in which the data identifying the signature means comprise data identifying:

- a signature method using the private key, and/or
- a memory medium on which said signature method is stored.

16. (New) A method according to claim 3, in which the data identifying hardware or a storage medium comprise:

- a reference identifying said hardware or said storage medium, and/or
- an identification of a manufacturer of said hardware or of said storage medium, and/or
- an indication of a security level of said hardware or of said storage medium defined according to a standard ISO 15408.

17. (New) A method according to claim 4, in which the data identifying hardware or a storage medium comprise:

- a reference identifying said hardware or said storage medium, and/or
- an identification of a manufacturer of said hardware or of said storage medium, and/or
- an indication of a security level of said hardware or of said storage medium defined according to a standard ISO 15408.

18. (New) A method according to claim 3, in which the data identifying a method comprise:

- a reference identifying said method, and/or
- an identification of an inventor of said method, and/or
- an indication of a security level of said method according to ISO 15408.

19. (New) A method according to claim 4, in which the data identifying a method comprise:

- a reference identifying said method, and/or
- an identification of an inventor of said method, and/or

- an indication of a security level of said method according to ISO 15408.

20. (New) A method according to claim 5, in which the data identifying a method comprise:

- a reference identifying said method, and/or
- an identification of an inventor of said method, and/or
- an indication of a security level of said method according to ISO 15408.